



LAUREA
AMMATTIKORKEAKOULU

Uuden edellä

Varmuuskopioinnin suunnittelu pk-yritykselle

Mäntysalo, Sampsa

2011 Leppävaara

Laurea-ammattikorkeakoulu
Leppävaara

Varmuuskopioinnin suunnittelu pk-yritykselle

Sampsa Mäntysalo
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Kesäkuu, 2011

Sampsa Mäntysalo

Varmuuskopioinnin suunnittelu pk-yritykselle

Vuosi 2011

Sivumäärä 43

Tämän työn tarkoituksena on selvittää ja toteuttaa GeoUnion Oy:lle sopiva varmuuskopiointimenetelmä. GeoUnion Oy on yksityinen geodesia-, geologia- ja geotekniikka-alan yritys. Yrityksen palveluihin kuuluu mittaus-, maaperätutkimus- ja suunnittelupalvelut. Yrityksellä on asiakkaita niin Suomessa kuin ulkomaillakin.

Työ aloitettiin selvittämällä yrityksen tarpeet ja vaatimukset varmuuskopiointimenetelmälle. Tämän jälkeen valittiin neljä näihin vaatimuksiin sopivaa varmistusmenetelmää, joita tutkittiin ja vertailtiin tarkemmin. Nämä menetelmät olivat nauha-asemat, etävarmistus, verkkokiintolevyt (NAS) ja kiintolevyt. Vertailu tehtiin tutkimalla menetelmien hyviä ja huonoja puolia, ja valinnan apuna käytettiin Kepner & Tregoen ongelmanratkaisumallia. Tutkimuksen tukena käytettiin alan kirjallisuutta ja verkkolähteitä. Tärkeimpänä lähteenä käytettiin yrityksen kehityspäällikön haastattelua. Haastattelu tehtiin kahdessa osassa. Ensimmäisessä osassa selvitettiin yrityksen tarpeet ja vaatimukset varmuuskopioinnille. Haastattelun toinen vaihe tehtiin sen jälkeen, kun varmuuskopiointi oli saatu käyntiin. Tämän tarkoitus oli selvittää, oltiinko yrityksessä tyytyväisiä valintaan.

Valittujen menetelmien vertailun tulokset käytiin läpi. Tutkimustulosten perusteella yritys valitsi itselleen sopivan menetelmän ja se otettiin käyttöön. Tutkimuksen aikana selvisi myös, että yrityksen palvelimen tallennuskapasiteetti alkoi olla lopussa. Tämä asia korjattiin samalla, kun varmuuskopiointi otettiin käyttöön.

Asiasanat: varmuuskopiointi, Nauha-asema, etävarmistus, verkkokiintolevy, kiintolevy, palvelin

Sampsa Mäntysalo

Designing and implementing a backup plan for middle-sized company

Year	2011	Pages	43
------	------	-------	----

The purpose of this thesis is to design and implement a backup plan for GeoUnion Oy. Geo Union Oy is a privately owned company that specializes in geodesy, geology and geotechnical engineering. The company's services include land surveying, soil research and planning services. The company has clients in Finland and abroad.

The thesis was started by investigating the needs and demands that the company had for backup. After that four methods were chosen and researched more closely. The four chosen methods were tape drives, online backup, network attached storage and hard drives. Methods were compared by benchmarking the pros and cons of the methods. The Kepner & Tregoe decision making model was also used in the process. The research was supported by literature and online publications on the subject. The most important source for the research was the interview of the company's development manager. The interview was conducted in two parts. The first part was used to discover the needs and demands the company had for backup. The second part was used to discover if the company had been satisfied with the choice.

When the research findings were ready the company chose one of the methods and that method is now in use. The research also revealed that the company's server storage capacity was almost full. This issue was also corrected when backup was implemented.

Keywords: backup, tape drive, online backup, network attached storage, hard drive, server

Sisällys

1	Johdanto	10
2	Kohdeyritys	11
2.1	Yrityksen tietoverkko	11
2.2	Nykyinen varmuuskopiointiratkaisu	12
2.3	Yrityksen varmuuskopioinnin tarve	12
3	Varmuuskopioinnin vaatimusmäärittely	13
3.1	Tavoitteet, kohderyhmät ja vaadittavat toiminnot	13
3.2	Varmuuskopioinnin merkitys	14
4	Varmuuskopiointi	15
4.1	Varmuuskopioinnin suunnittelu	16
5	Tietojen varmistaminen ja tietoturva	16
6	Varmuuskopiointimenetelmät	18
6.1	Nauha-asemat ja nauhat	18
6.2	Nauhaformaatit	19
6.2.1	DDS	19
6.2.2	DLT	19
6.2.3	SDLT	20
6.2.4	AIT	20
6.2.5	SAIT	21
6.2.6	LTO	21
6.3	Etävarmistus	22
6.4	Kiintolevyt	23
6.4.1	Kiintolevyjen liitännät	23
6.4.2	IDE	23
6.4.3	SATA	24
6.4.4	SCSI	25
6.5	Verkkokiintolevyt	25
7	Tutkittujen vaihtoehtojen vertailu	27
7.1	Varmistustekniikoiden benchmarking vertailu	27
7.1.1	Etävarmistus	27
7.1.2	Nauha-asemat ja nauhat	28
7.1.3	Verkkokiintolevyt	29
7.1.4	Kiintolevyt	30
7.2	Varmistustekniikoiden Kepner & Tregoe vertailu	31
7.3	Kepner & Tregoe vertailun tulokset	32
7.4	Päätösanalyysi	32
8	Ratkaisuehdotus	33

9	Valittu ratkaisu ja kustannukset	34
10	Kehitysprojektin yhteenveto	35
	Kuvat	38
	Taulukot	39
	Liitteet	40

SYMBOLI- JA TERMILUETTELO

AIT	Nauhataallennuksessa käytetty magneettinauha
Blu-ray-levy	Optisen datan tallennusväline
CD-levy	Optisen datan tallennusväline
DDS	Nauhataallennuksessa käytetty magneettinauha
DLT	Nauhataallennuksessa käytetty magneettinauha
DVD-levy	Optisen datan tallennusväline
Fibre channel	Kokoelma standardeja, jotka määrittelevät yhtenäisen tavan siirtää tietoa tietokoneiden ja oheislaitteiden välillä.
FireWire	Ulkoisten oheislaitteiden liitäntästandardi, joka mahdollistaa erittäin nopean tiedonsiirron.
Gigatavu	Tietotekniikassa käytetty tallennuskapasiteetin yksikkö
IDE	Kiintolevyjen ja optisten asemien liitäntäväylä
LTO	Nauhataallennuksessa käytetty magneettinauha
Magneettinauha	Magneettisella materiaalilla, usein rautaoksilla päällystetty muovinauha, jota käytetään datan tallennukseen.
Megatavu	Tietotekniikassa käytetty tallennuskapasiteetin yksikkö
NAS	Tallennusjärjestelmä, joka jakaa tiedostoja verkossa yhteiskäyttöön.

Palvelin	Tietoliikenteen yhteydessä tietokoneessa suoritettava palvelinohjelmisto tai tämänlaista ohjelmistoa pyörittävä tietokone.
RAID	Tekniikka, jolla tietokoneiden vikasietoisuutta ja/tai nopeutta kasvatetaan käyttämällä useita erillisiä kiintolevyjä, jotka yhdistetään yhdeksi loogiseksi levyksi.
Rpm	Pyörimisnopeuden yksikkö
SAIT	Nauhatalennuksessa käytetty magneettinauha
SATA	Sarjamuotoinen liitäntä sisäisen tai ulkoisen massamuistilaitteen, kuten kiintolevyn liittämiseen tietokoneeseen.
SCSI	Standardi tiedon välittämiseen tietokoneen ja oheislaitteiden välillä
SDLT	Nauhatalennuksessa käytetty magneettinauha
Teratavu	Tietotekniikassa käytetty tallennuskapasiteetin yksikkö
UPS-laite	Yleisimmiltä sähköverkon häiriöiltä kuten sähkökatkoksilta sekä lyhyt- että pitkäaikaisilta ali- ja ylijännitteiltä suojaava laite.
USB	Sarjamuotoinen väylä, jonka kautta tietokone ja oheislaitteet voivat kommunikoida keskenään.
Windows Server 2003	Microsoftin julkaisema palvelinkäyttöjärjestelmäohjelmisto
Windows XP	Microsoftin kehittämä käyttöjärjestelmä tietokoneisiin

WLAN

Langaton lähiverkkotekniikka, missä erilaiset verkkolaitteet voidaan yhdistää ilman kaapeleita.

1 Johdanto

Nykypäivän tietomäärät kasvavat kovaa vauhtia tekniikan kehittyessä ja tämä on johtanut säilytettävien tietomäärien nopeaan kasvuun. Yritysten tietoverkkojen sisältämät datamäärät kasvavat jatkuvasti, mikä aiheuttaa ongelmia yrityksille tiedon varastoinnissa. Tietomäärien nopean kasvun lisäksi ongelmia aiheuttaa tiedon säilyttämisvelvollisuuden pituus.

Tiedon säilyttämisessä on olennaista tiedon varmuuskopiointi. Tämän takia nykyinen työnantajani on pyytännyt, että tutkin yritykselle erilaisia vaihtoehtoja varmuuskopioinnin toteuttamiseen. Tutkimuksen perusteella yritys valitsee itselleen sopivan menetelmän ja ottaa sen käyttöön.

Varmuuskopioinnin tarpeeseen vaikuttaa oleellisesti se, että yrityksellä olevien palvelinten tallennuskapasiteetti on loppumassa. Tähän on vaikuttanut yritykseen ostettu uusi mittauslaite, jonka tuottamat datamäärät vievät paljon tilaa. Tälle datalle on varattu kokonaan oma tallennustila, mutta sekin alkaa olla täynnä eikä vanhojen projektien tietoja voida poistaa, koska niistä ei ole varmuuskopioita. Toinen vaikuttava tekijä on se, että yrityksen tiedonsäilyttämisvelvollisuus on 10 vuotta. (KSE 1995 2010).

Varmuuskopioitavan datan määrän takia valittiin neljä vaihtoehtoista tallennusmenetelmää, jolle kopioita voisi alkaa tehdä. Nämä ovat nauhatalennus, etävarmistus ja ulkoiset - ja verkkokiintolevyt. Nauhatalennus valittiin myös sen takia, että yritykseen on aikoinaan ostettu nauha-asema, mutta sitä ei ole otettu koskaan käyttöön. CD,- DVD- ja Blu Ray-levyjen tallennuskapasiteetti jää auttamatta liian pieneksi, joten ne olen jättänyt tutkimuksen ulkopuolelle. Niiden avulla kopioiden tekeminen olisi myös työlästä. Yrityksen toiveena on, että varmuuskopioinnista saadaan mahdollisimman vaivaton ja automaattisesti toimiva. Sopivan menetelmän löytämiseksi apuna käytetään avointa haastattelua, jonka avulla rajataan yrityksen tarpeet ja vaatimukset varmistusmenetelmälle (Liite 1, osa 1).

2 Kohdeyritys

Kohdeyrityksenä toimii GeoUnion Oy. GeoUnion Oy on yksityinen geodesia-, geologia- ja geotekniikka-alan yritys. Yrityksen palveluihin kuuluu mittaus-, maaperätutkimus- ja suunnittelupalvelut. Työntekijöitä yrityksellä on noin 30, joista noin puolet työskentelee erilaisissa projekteissa eri puolilla Suomea ja puolet Helsingin toimipisteessä. Työntekijöiden määrä vaihtelee projektien mukaan. Yrityksellä on kaksi toimipistettä, yksi Helsingissä ja toinen Malesiassa. Tämä tutkimus painottuu pääasiallisesti Helsingin toimipisteeseen.

Yrityksen palveluihin kuuluu kahdeksan erilaista tuoteryhmää:

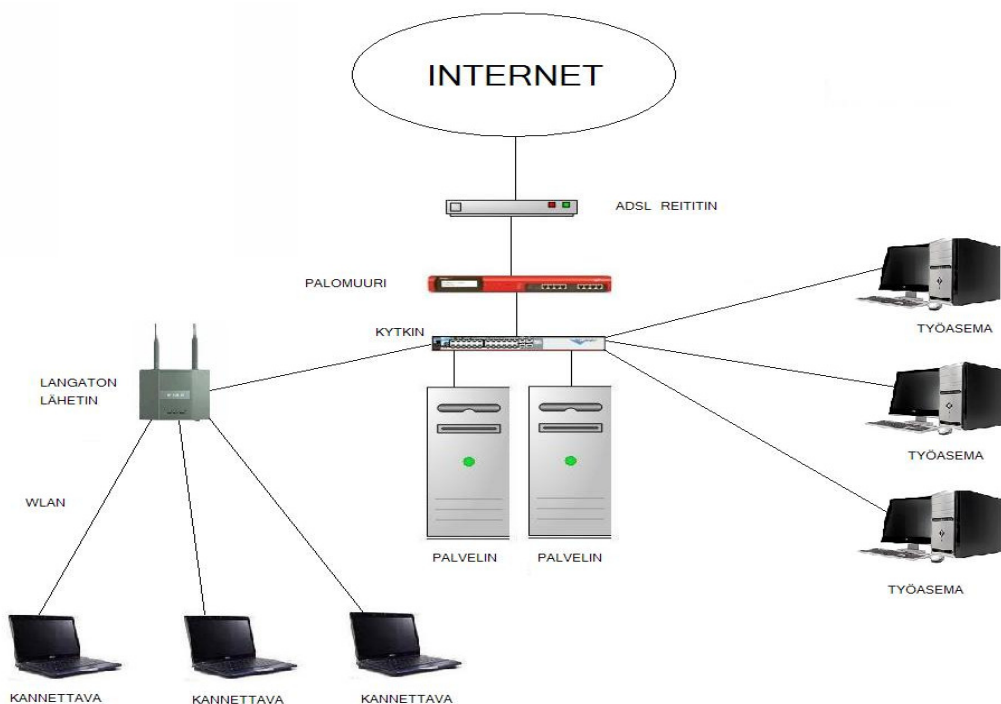
- pohjatutkimukset
- maanrakentamisen valvonta
- maalaboratorio
- mittaus
- geotekninen suunnittelu
- geologinen suunnittelu
- kunnallistekninen suunnittelu
- urheilu- ja liikunta-alueiden rakennussuunnittelu

(GeoUnion Oy 2010).

2.1 Yrityksen tietoverkko

Helsingin toimipisteen tietoverkko koostuu kahdesta palvelimesta ja noin viidestätoista työasemasta. Työasemat toimivat pääasiassa Windows XP -käyttöjärjestelmällä. Työasemat ovat yhteydessä sisäverkkoon kaapelilla tai langattomasti WLAN-yhteydellä. Yrityksen tietoverkon ylläpidosta vastaa siihen palkattu ICT-yritys (Kuva 1).

Palvelimet ovat HP Proliant ML 350-sarjan palvelimia. Toinen palvelimista pyörittää Helsingin toimiston sisäverkkoa ja pitää sisällään 3 verkko-asemaa. Verkko-asemia käytetään töihin liittyvien aineistojen ja taloushallinnon asiakirjojen säilytykseen. Käyttöjärjestelmänä palvelimessa on Windows Server 2003. Toista palvelimista (Scanserver) käytetään yhteisenä tallennustilana ja tiedon siirtoa varten Helsingin ja Malesian toimipisteiden kesken.



Kuva 1: Geo Union Oy:n tietoverkon rakenne.

2.2 Nykyinen varmuuskopointiratkaisu

Tällä hetkellä yrityksessä tehdään varmuuskopiointia käyttäjien palvelimella sijaitsevista kansioista ja sähköposteista. Nämä varmistukset tehdään verkon yli yrityksen it-tuesta vastaavan yrityksen toimesta. Sisäverkkoa pyörittävästä palvelimesta ja sen sisältämistä verkkolevyistä tehdään varmistukset palvelimeen liitetylle ulkoiselle kovalevyille. Palvelimen käyttöjärjestelmästä on myös tehty palautuslevy niin, että järjestelmä pystytään palauttamaan sen kaatuessa. Scanserver-palvelimen tiedoista on projekteja pakattu ja poltettu DVD-levyille ja vanhimmat projektit on kopioitu ulkoiselle kovalevyille. Uusimmista projekteista ei ole kopioita ollenkaan, vaan ne sijaitsevat vain palvelimella. Data koostuu valokuvista, pdf-tiedostoista, tekstitiedostoista ja maanmittaukseen ja suunnitteluun tarkoitettujen ohjelmien ja laitteiden tuottamasta datasta.

2.3 Yrityksen varmuuskopioinnin tarve

Varmuuskopioitavan tiedon määrä on tällä hetkellä noin 750 gigatavua. Toisella palvelimella on kolme verkkolevyä, jotka ovat 100 gigatavun kokoisia. Nämä verkkolevyt alkavat olla täynnä ja lisätilan hankkiminen alkaa olla ajankohtaista. Scanserver-palvelimen tallennuskapasiteetti on yhteensä 3300 gigatavua. Tästä on Helsingin toimipisteen käytössä 880 gigatavua, josta noin puolet on käytössä. Varmuuskopioinnin tarve on suuri, sillä

kunnollista varmistusta ei ole tehty. Kopiot sijaitsevat yrityksen tiloissa ja esimerkiksi tulipalon sattuessa lähes kaikki tiedot voisivat tuhoutua.

3 Varmuuskopioinnin vaatimusmäärittely

3.1 Tavoitteet, kohderyhmät ja vaadittavat toiminnot

GeoUnion Oy:n varmuuskopioinnissa on ollut puutteita jo pitkän aikaa. Suunnitelmana on tutkia erilaisia varmuuskopiointimenetelmiä ja valita niistä yritykselle sopiva menetelmä. Mahdollisista menetelmistä on valittu neljä, joita tutkitaan tarkemmin. Nämä menetelmät ovat nauha-asemat, etävarmistus, ulkoiset kiintolevyt ja verkkokiintolevyt. Menetelmät on valittu siksi, että kaikille niistä on mahdollista helposti varmistaa suuria tietomääriä, niiden tallennuskapasiteettia on helppo kasvattaa ja varmistus mahdollista tehdä niille automaattiseksi. Tärkeimmät kriteerit valinnalle ovat helppokäyttöisyys, luotettavuus, laajennettavuus ja kustannukset.

Kohderyhmänä toimivat:

- yrityksen työntekijät
- GeoUnion Oy:n verkkoa ylläpitävä yritys
- mahdollinen ulkopuolinen yritys, jolta palvelu tilataan.

Haastattelun avulla selvitettiin yrityksen vaatimat ominaisuudet varmuuskopioinnille. Yritys vaatii varmuuskopiointimenetelmältä seuraavia ominaisuuksia:

- helppokäyttöisyyttä
- luotettavuutta
- turvallisuutta
- laajennettavuutta
- muokattavuutta
- toipumista virhetilanteista.

(Liite 1, osa 1).

Helppokäyttöisyyttä vaaditaan siksi, että menetelmän täytyy olla niin yksinkertainen, että tarvittaessa yrityksen työntekijä pystyy palauttamaan varmistettua tietoa. Luotettavuutta vaaditaan, koska yritys haluaa, että valitun menetelmän toimintaan voidaan luottaa.

Turvallisuutta vaaditaan, koska valitun menetelmän halutaan olevan turvallinen.

Laajennettavuutta vaaditaan, koska varmistettavan tiedon määrä tulee kasvamaan ja varmistusmenetelmän tallennuskapasiteettia täytyy pystyä tulevaisuudessa kasvattamaan.

Muokattavuudella tarkoitetaan sitä, että valittu menetelmä on helppo liittää, jos esimerkiksi tietoverkon rakenne muuttuu. Menetelmän halutaan myös pystyvän toipumaan mahdollisista virhetilanteista.

3.2 Varmuuskopioinnin merkitys

Varmuuskopioinnin avulla parannetaan yrityksen toimintaa turvaamalla tärkeiden tiedostojen säilyminen. Täysin aukotonta varajärjestelyä ei kuitenkaan ole, vaan siihen liittyy aina riskejä. Tämän takia tiedon varmistamiseen liittyen on tehtävä riskianalyysi. Analyysin avulla kartoitetaan mahdolliset riskit ja niiden todennäköisyys ja seuraukset. Analyysissa käytetään arvoasteikkoa 1-5, jossa 1 = merkityksetön riski ja 5 = sietämätön riski. (Kuusela & Ollikainen 2005, 242-272).

Seuraavaksi listataan mahdolliset riskit, joihin voidaan törmätä ennen varmistusta, sen aikana ja sen jälkeen. Riskejä ovat muun muassa:

- tiedot tuhoutuvat ennen varmistusta
- varmuuskopiointi ei toimi
- varmistusten palautus ei onnistu
- varmistustekniikka vanhenee
- varmistamiseen käytettävä laite hajoaa.

Tietojen tuhoutuminen ennen varmistusta on tällä hetkellä kohtalainen riski, koska kunnollista varmistusta ei ole tehty. Esimerkiksi tulipalo olisi kohtalokas tapahtuma ennen varmistuksen aloittamista. Varmuuskopiointi tullaan toteuttamaan melko uudella tekniikalla, joten sen toimimattomuus on riskinä vähäinen. Varmistusten palauttamisessa voi myös tulla ongelmia. Ohjelmat päivittyvät nopeasti ja tämä voi aiheuttaa sen, että vanhoja tiedostoja ei saa enää auki uudemmilla ohjelmaversioilla. On myös mahdollista, että esimerkiksi jokin tiedosto korruptoituu eikä sitä saa enää avattua. Tekniikka kehittyy nopeasti ja laitteet ja menetelmät muuttuvat, mikä aiheuttaa riskin tietojen varmistamiselle ja palauttamiselle. Laitevika on aina mahdollinen riski, kun kyseessä tietotekninen laite tai menetelmä. Riskitaulukosta voi päätellä, että tapahtumien todennäköisyys on kohtalaista tai vähäistä, mutta tapahtuman seuraukset ovat aina merkittäviä tai jopa sietämättömiä (Taulukko 1).

Riski	Tapahtuman todennäköisyys	Tapahtuman seuraukset
Tiedot tuhoutuvat ennen varmistusta	3	5
Varmuuskopiointi ei toimi	2	5
Varmistusten palautus ei onnistu	3	4
Varmistustekniikka vanhenee	2	4
Varmistamiseen käytettävä laite hajoaa	3	4

1 = Merkityksetön riski
 2 = Vähäinen riski
 3 = Kohtalainen riski
 4 = Merkittävä riski
 5 = Sietämätön riski

Taulukko 1: Riskit.

4 Varmuuskopiointi

Varmuuskopiointi tarkoittaa olemassa olevien tiedostojen kopiointia siltä varalta, että alkuperäinen kopio tuhoutuu. Varmuuskopioinnin avulla tiedot voidaan palauttaa ja työskentelyä voidaan jatkaa siitä, mihin jäätiin ennen kopion tekemistä.

Varmuuskopiot voidaan jakaa viiteen eri ryhmään:

- normaali
- kopiointi
- erotus (differential)
- lisäys (incremental)
- päivittäinen.

Normaalissa varmuuskopioinnissa kaikki tiedostot kopioidaan ja merkitään varmuuskopioiduiksi. Kopioinnissa kaikki tiedostot kopioidaan, mutta niitä ei merkitä kopioiduiksi. Erotuksessa kaikki edellisen varmuuskopioinnin jälkeen muuttuneet tiedostot kopioidaan, mutta ei merkitä varmuuskopioiduiksi. Lisäyksessä kaikki edellisen varmuuskopioinnin jälkeen muuttuneet tiedostot kopioidaan ja merkitään varmuuskopioiduiksi. Päivittäinen varmuuskopiointi kopioi kaikki kyseisen päivän aikana

muuttuneet tiedostot, mutta ei merkitse niitä varmuuskopioituiksi. (Ruohonen 2002, 209-219; Paavilainen 1998, 220-224).

4.1 Varmuuskopioinnin suunnittelu

Varmuuskopioinnin suunnittelussa tulee ottaa huomioon seuraavat asiat:

- halutuista tiedoista otetaan kopiot riittävän usein
- varmuuskopiointi voidaan suorittaa käytettävissä olevassa ajassa
- varmuuskopioidut tiedostot voidaan palauttaa riittävän nopeasti.

Varmuuskopioiden säilyttäminen sisältää erilaisia riskejä. Varmuuskopiot tulisi säilyttää paikassa, jossa ne eivät tuhoudu alkuperäisen kopion mukana. Yritysten varmuuskopioinnissa tulisi ottaa huomioon myös sellaiset riskit kuten varkaus, tulipalo tai jopa luonnonmullistukset. Myös magneettiset häiriöt tulee ottaa huomioon, jos varmuuskopiot on tallennettu magneettisesti, esimerkiksi kovalevyille tai magneettinauhalle. Näiden syiden takia yrityksen varmuuskopiot tulisi säilyttää toisessa rakennuksessa tai esimerkiksi tulenkestävässä kassakaapissa ja useana eri kopiona. Varmuuskopioinnin onnistuminen tulee myös tarkistaa määräajoin. (Ruohonen 2002, 209-219, Paavilainen 1998, 220-224).

5 Tietojen varmistaminen ja tietoturva

Tietoturva ja tietojen varmistaminen kuuluvat oleellisesti yhteen. Tietoturva kattaa kaiken, mikä liittyy tietojen saatavuuteen, oikeellisuuteen sekä tietojen luottamuksellisuuteen käsittelyn, säilytyksen ja tiedonsiirron aikana. Tietoturva tarjoaa erilaisia keinoja ja toimintamalleja tietosuojan ylläpitämiseen.

Tietoturva koostuu kolmesta osa-alueesta, jotka muodostavat tietoturvallisuuden perustan (CIA). Tietoturvan tavoitteena on taata tiedon:

- luottamuksellisuus (confidentiality)
- eheys (integrity)
- saatavuus (availability).

Tiedon luottamuksellisuus tarkoittaa sitä, että tietoa ei pääse käsittelemään kukaan kenellä ei ole siihen oikeutta. Toisin sanoen tietoa voivat lukea tai muokata vain ne, joille on annettu siihen oikeus etukäteen. Tiedon eheys tarkoittaa sitä, että tiedon sisältö ei ole muuttunut minkään ulkopuolisen tahon kautta. Tämä tarkoittaa esimerkiksi tiedostojen poistamista tai muuttamista. Tämän voi aiheuttaa esimerkiksi virus tai tahattomasti levyille tullut vika-alue.

Tiedon saatavuus tarkoittaa sitä, että tieto on saatavilla silloin, kun sitä tarvitaan. Tärkein tekijä saatavuuden varmistamiseen on tiedostojen varmuuskopiointi sekä laitteiden toimintaa turvaava tekniikka, esimerkiksi UPS-laite sähkökatkojen varalta.

Näiden kolmen osa-alueen lisäksi tietoturva edellyttää kolmen muun periaatteen toteutumista. Nämä ovat todentaminen (authentication), pääsynvalvonta (access control) ja kiistämättömyys (non-repudiation).

Luottamuksellisuuden toteutuminen edellyttää todentamista. Todentamisen (authentication) avulla varmistutaan olion aitoudesta. Olio voi olla esimerkiksi käyttäjä. Käyttäjän todennukseen käytetään tietojärjestelmissä yleensä salasanaa tai käyttäjätunnuksen ja salasanan yhdistelmää.

Pääsynvalvontaa valvoo käyttöjärjestelmä. Geo Union Oy:n tapauksessa tämä käyttöjärjestelmä on Windows Server 2003. Käyttöjärjestelmä valvoo, että vain todennetut henkilöt pääsevät järjestelmän tietoihin. Pääsynvalvontaan kuuluu myös käytön seuranta (audit). Järjestelmään tallentuu tietoa käyttäjistä. Näitä tietoja voidaan jälkeenpäin tutkia ja käyttää esimerkiksi mahdollisen tietoturvarikkomuksen selvittämisessä.

Kiistämättömyys (non-repudiation) on kauppatahtumaan liittyvä vaatimus. Se saavutetaan soveltamalla tiedon eheyteen ja todennukseen liittyviä periaatteita. Kiistämättömyydellä varmistetaan se, että kauppatahtumaan osallistuneiden osapuolten osallisuus voidaan jälkeenpäin varmentaa. (Järvinen 2002, 21-28, Hakala, Vainio & Vuorinen 2006, 4-12, Paavilainen 1998, 4-12 ja 23-25).

6 Varmuuskopiointimenetelmät

6.1 Nauha-asetat ja nauhat

Nauha-asema on tallennusväline, joka lukee ja kirjoittaa magneettinauhalle tai reikänauhalle tallennettua tietoa. Nauha-asetama käytetään tyypillisesti kiintolevyille tallennetun tiedon arkistointiin. Nauha-asetmien tärkeä ominaisuus on se, että nauhan pystyy helposti viemään fyysisesti toiseen paikkaan ja näin turvaamaan tiedon säilymisen. Nauha-asetman etuna on myös, että tietoa saa talletettua nopeasti suuria määriä. Esimerkiksi LTO-asetmat pystyvät siirtämään dataa yli 250 megatavua sekunnissa (myöhemmin MB/s. (LTO 4) (Kuva 2).

Muistit jaetaan niiden saatitavan mukaan kahteen luokkaan, sarjasaantimuisteihin ja suorasaantimuisteihin. Nauha-asetmien käyttämä muisti on sarjasaantimuistia. Tämä tarkoittaa sitä, että tiedon saaminen nauhalta on hitaampaa kuin esimerkiksi suorasaantimuistilla toimivalta kiintolevyiltä. Sarjasaantimuisteissa koko nauhan muisti voidaan joutua lukemaan läpi halutun tiedon löytymiseksi. Suorasaantimuisteissa esimerkiksi kiintolevyissä luku-/kirjoituspää pystyy nopeasti liikkumaan mihin tahansa satunnaiseen kohtaan levyllä hyvin lyhyessä ajassa ja näin ollen löytämään halutun tiedon nopeammin.

Nauha-asetman voi liittää tietokoneeseen SCSI-, Fibre channel-, IDE-, USB-, FireWire tai muun liittynnän kautta. Nauha-asetmien tallennuskapasiteetti on muutamasta megabitistä teratavuihin. Nauhojen kapasiteetista puhuttaessa käytetään kahta eri määritelmää, natiivi ja pakattu. Natiivi tallennuskapasiteetti kertoo sen määrän mitä nauhalle mahtuu tietoa ilman pakkaamista ja pakattu sen mikä on nauhan tallennuskapasiteetti, kun data pakataan. Nauhojen kapasiteetti saadaan tuplattia pakkaamalla data nauhalle suhteella 2:1. (Hewlet & Packard 2010)



Kuva 2: HP:n Storageworks Ultrium nauha-asetama.

6.2 Nauhaformaatit

Magneettinauhaa on käytetty tiedon tallennukseen jo 50 vuotta. Tässä ajassa nauhat ovat kehittyneet paljon. Varmuuskopiointiin tarkoitettut nauhat alkoivat kehittyä 1980-luvulla.

Nauhaformaatit jakautuvat valmistajan ja tallennuskapasiteetin mukaan. Formaateista löytyy myös eri versioita, joten nauhan valitsemisessa kannattaa olla tarkka. Nauha-asemat eivät välttämättä lue eri valmistajien nauhoja tai lukevat vain tiettyä versiota nauhasta.

6.2.1 DDS

Digital Data Storage (DDS) on Sonyn ja Hewlet Packardin vuonna 1989 kehittämä nauhatallennusmedia. Se kehitettiin Digital Audio Tape-teknologiasta (DAT). DDS:n suuri etu oli sen pieni koko ja suuri tallennuskapasiteetti. DDS:tä kehitettiin 4 versiota (DDS4), jonka jälkeen se päätettiin lopettaa. Hewlet Packard kuitenkin julkaisi vuonna 2003 DAT72-formaatin, koska DDS-formaatin lopettaminen jätti markkinat samalla tekniikalla toimiville nauhoille (Sony 2010) (Kuva 3).

Format	DAT	Date	Tape Length (m)	Capacity (GB)	Speed (MB/s)
DDS-1	DAT	1989	60/90	1.3/2.0	0.18
DDS-2	DAT-8	1993	120	4.0	0.6
DDS-3	DAT-24	1996	125	12.0	1.1
DDS-4	DAT-40	1999	150	20.0	3.2
DDS-5	DAT-72	2003	170	36.0	3.2
DDS-6	DAT-160	2007	154	80	6.9

Kuva 3: Kaavio DDS:n tiedonsiirtonopeuden kehitymisestä.

6.2.2 DLT

Aikaisemmin Compact Tape nimellä tunnettu Digital Linear Tape (DLT) on 1984 kehitetty magneettinauha. Sen kehitti Digital Equipment Corporation (DEC), ja Quantum Corporation osti teknologian 1994. Ensimmäiselle vuonna 1984 julkaistulle versiolle pystyi tallentamaan 94 megatavua. 1989 julkaistulle versiolle pystyi tallentamaan jo 2.6 GB. DLT:n kehittyneempi versio Super Digital Linear Tape (SDLT) julkaistiin 2001. Sen tallennuskapasiteetti oli parhaimmillaan 110 GB. (Quantum Corporation).

6.2.3 SDLT

Super Digital Linear Tape (SDLT) on kehittyneempi versio DLT-formaatista. SDLT:n suuri tallennuskapasiteetti ja nopea tiedonsiirtonopeus lisäsivät sen suosiota. SDLT-nauhoja pystyi myös lukemaan DLT-nauhoille sopivilla nauha-asemilla eli DLT-nauhoja käyttäneen yrityksen ei tarvinnut hankkia uutta nauha-asemaa käyttääkseen SDLT-nauhoja. Ensimmäinen SDLT-sukupolvi tarjosi 110 gigatavun tallennuskapasiteetin ja kolmas sukupolvi (SDLT2) 320 gigatavua ja 32 MB/s siirtonopeuden (McIntosh 2009) (Kuva 4).



Kuva 4: Super Digital Linear Tape.

6.2.4 AIT

Sony julkaisi vuonna 1996 Advanced Intelligent Tape -formaatin (AIT) kilpailijaksi jo olemassa oleville DAT/DDS - ja DLT formaateille. AIT -formaatti suunniteltiin päivitysvaihtoehdoksi DDS3-formaatilla toimiville järjestelmille. AIT:n ensimmäinen versio tarjosi 25 gigatavua tallennustilaa.

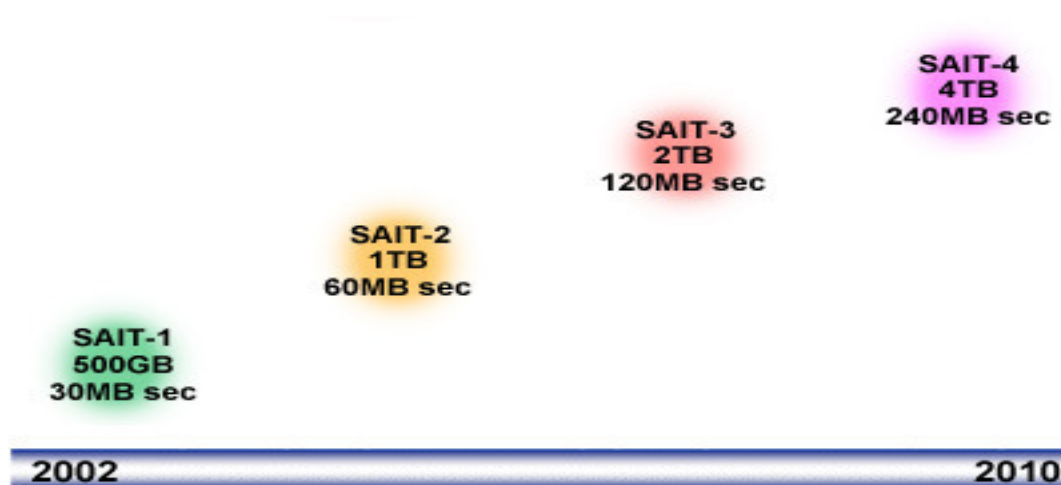
1999 julkaistun AIT-2-formaatin tallennuskapasiteetti oli 50 gigatavua. Suuremman tallennuskapasiteetin lisäksi formaattiin kehitettiin uusi tärkeä ominaisuus nimeltä WORM (Write Once Read Many). Ominaisuus oli tärkeä uudistus pitkäaikaiseen tiedon varastointiin. Ominaisuuden takia tallennettua tietoa ei pystynyt jälkeenpäin muokkaamaan tai vahingossa poistamaan, minkä takia se oli haluttu ominaisuus varmuuskopiointiin. AIT-4 julkaistiin vuonna 2005, ja sen tallennuskapasiteetti oli 200 gigatavua ja tiedonsiirtonopeus 24 MB/s (Kuva 5) (PCTECHGUIDE).

	AIT-1	AIT-2	AIT-3	S-AIT
Native Capacity	35GB	50GB	100GB	500GB
Compressed Capacity	90GB	130GB	260GB	1.3TB
Native DTR	4MBps	6MBps	12MBps	30MBps
Compressed DTR	10MBps	15.6MBps	31.2MBps	78MBps
Form Factor	3.5in	3.5in	3.5in	5.25in
Media Type	8mm AME	8mm AME	8mm AME	1/2in AME
MTBF (hours)	300,000	300,000	400,000	500,000

Kuva 5: Kaavio AIT:n kehityksestä.

6.2.5 SAIT

2004 Sony julkaisi kehittyneemmän version AIT:stä nimeltä Super Advanced Intelligent Tape (SAIT). SAIT oli ensimmäinen formaatti, jonka tallennuskapasiteetti pakattuna ylitti 1 teratavun kapasiteetin. SAIT nauhoja on mahdollista myös saada WORM ominaisuudella varustettuna (Kuva 6) (PCTECHGUIDE).

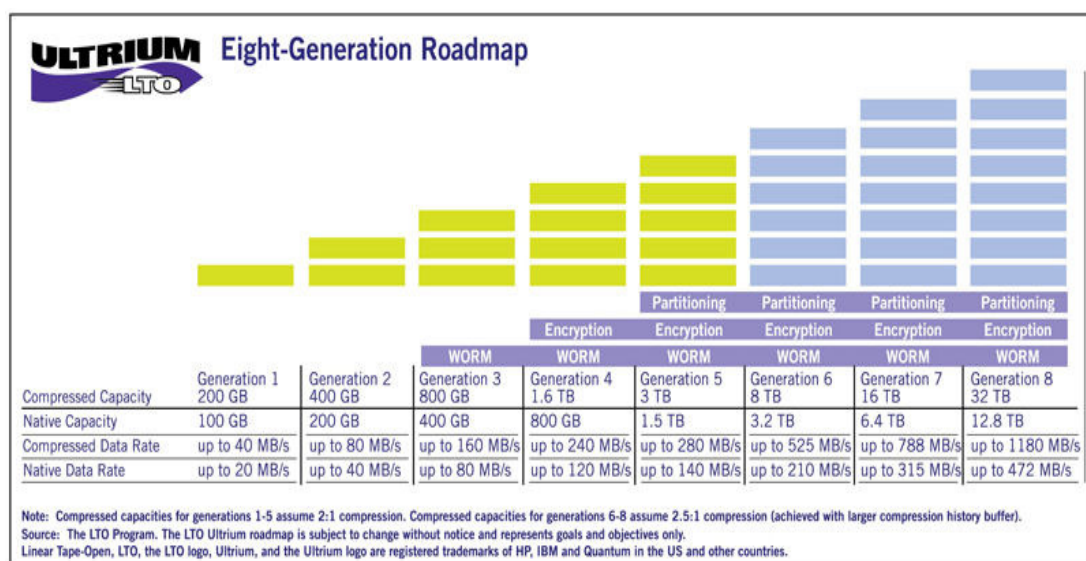


Kuva 6: SAIT:n kehittyminen.

6.2.6 LTO

Linear Tape Open (LTO) on HP:n, IBM:n ja Quantumin kehittämä tallennusmenetelmä. LTO-tekniikka tunnetaan nykyään nimellä LTO Ultrium, jonka ensimmäinen versio LTO julkaistiin vuonna 2000 ja siihen pystyi tallentamaan 100GB natiivia dataa ja 200 gigatavua pakattua dataa per nauha. LTO Ultriumista on tähän mennessä julkaistu viisi versiota ja uusimmalle

2010 julkaistulle LTO 5-versiolle pystyy tallentamaan 3 teratavua pakattua dataa. (ULTRIUM LTO) (Kuva 7).



Kuva 7: LTO-tekniikan suunniteltu kehittyminen.

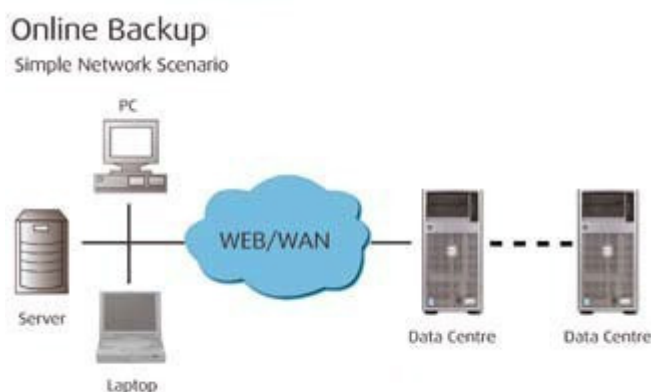
6.3 Etävarmistus

Etävarmistus on palvelu, jonka avulla varmuuskopiot tiedostoista ja järjestelmästä tehdään tietoverkon yli etäyhteydellä. Etävarmistuksen hoitaa yleensä toinen yritys, joka myy kyseistä palvelua. Palvelun tarjoaja ottaa etäyhteyden yrityksen järjestelmään ja kopioi sieltä sovitut tiedostot. Tyypillisiä etävarmistukseen liittyviä ominaisuuksia ovat tiedostojen kopionti (vaikka ne olisivat käytössä), tiedon salaus, monen eri toimipisteen varmuuskopiointi ja varmuuskopioituille tiedostoille pääsy käyttäen internet-selainta. Usein aluksi tehdään normaali kopio eli kaikki tiedostot kopioidaan ja sen jälkeen kopioidaan vain muuttuneet ja uudet tiedostot. (Kuva 8.)

Etävarmistuksen hinta koostuu seuraavista asioista:

- kopioitavan tiedon määrä
- varmuuskopioitavien tietokoneiden/palvelinten määrä
- säilytettävien kopioiden määrä
- tietojen säilyttämisen pituus
- mahdollinen käyttöönottopalvelu.

(Järvinen 2002, 58-59, SearchStorage.com 2010).



Kuva 8: Esimerkki etävarmistuksen toteutuksesta.

6.4 Kiintolevyt

Kiintolevy on tietokoneeseen kiinteästi tai ulkoisesti liitetty massamuisti. Kiintolevylle asennetaan tietokoneen käyttöjärjestelmä ja ohjelmat ja sitä käytetään tiedostojen tallennukseen. Tieto tallentuu kiintolevylle magneettisesti. Tieto tallentuu bitti kerrallaan jonoihin ympyrän muotoisille urille. Magneettikenttiin tallennettu data saadaan sähköiseksi, kun lukupään ohi kulkeva magneettinen varaus indusoi siihen sähkövirran. Virran muutokset tulkitaan signaaleiksi, jotka muutetaan ohjauselektronikan avulla käyttökelpoiseen muotoon.

Kiintolevyjen tallennuskapasiteetti on laaja. Kapasiteetti on mahdollista saada sadoista megatavuista aina kahteen teratavuun asti. Kiintolevyn tärkeä ominaisuus on sen pyörimisnopeus. Työasemien kiintolevyjen pyörimisnopeus vaihtelee 7200 rpm - 15 000 rpm (Revolutions per minute). Kannettavissa tietokoneissa pyörimisnopeus on hitaampi, 4200 - 5400 rpm. Mitä nopeampi pyörimisnopeus sitä nopeammin teoriassa tietokone pääsee käsiksi tietoon ja tämän takia toimii nopeammin. (MANUAALI.FI, PCGUIDE).

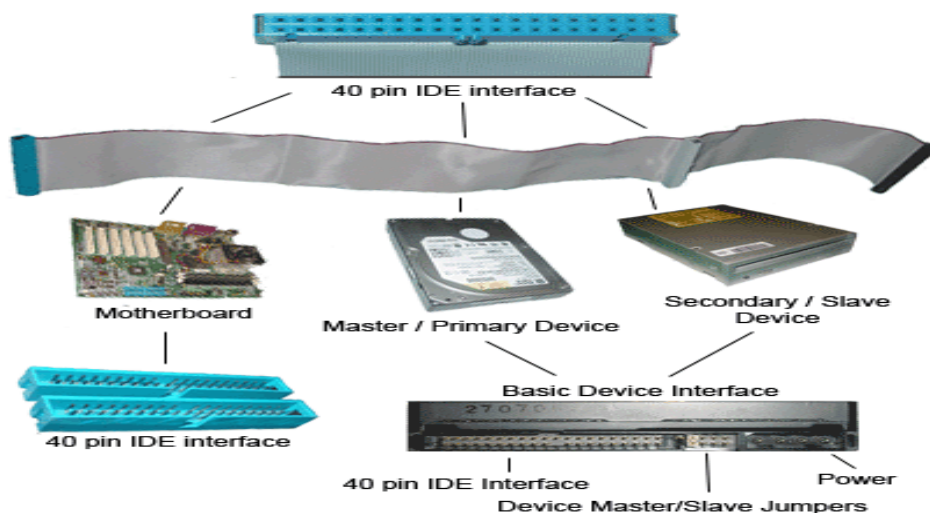
6.4.1 Kiintolevyjen liitännät

Yleisimmät kiintolevyn liitännät ovat IDE/ATA, SATA ja SCSI. Kiintolevy on mahdollista liittää yleensä useammalla tavalla ja tämä takaa niille hyvän liitettävyyden. Seuraavaksi esitellään kiintolevyjen erilaiset liitännät.

6.4.2 IDE

IDE (Integrated Drive Electronics) on kiintolevyjen ja optisten asemien liitäntäväylä. IDE tunnetaan myös nimillä EIDE (Enhanced IDE), ATA (AT Attachment) ja PATA (Parallel AT Attachment). Liityntäväylän kautta data kulkee rinnakkaisesti 16 bittiä kerrallaan.

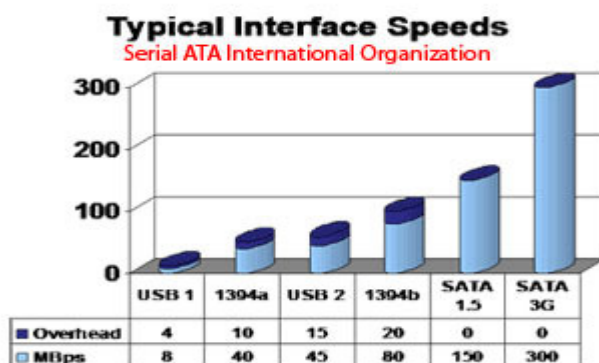
Ensimmäisen version tiedonsiirtonopeus oli 16 MB/s ja uusimman version 133 MB/s. Vuoden 2007 alusta alkaen IDE-liityntävyä on alettu korvata SATA-liitynnällä (Serial ATA). (KnowledgeRush) (Kuva 9).



Kuva 9: IDE:n liitännät ja liittäminen tietokoneeseen.

6.4.3 SATA

SATA (Serial ATA) on sarjamuotoinen liitäntä sisäisen tai ulkoisen massamuistilaitteen, kuten kiintolevyn liittämiseen tietokoneeseen. Toisin kuin sen edeltäjä IDE, SATA käyttää tiedon siirtämiseen sarjamuotoista tiedonsiirtoa. Tämä tekee SATA kaapeleista paljon kapeampia ja halvempia valmistaa. Tiedonsiirtonopeus on myös oleellisesti kehittynyt jo SATA 1.0-versiossa nostaen nopeuden 150 MB/s. Uusimmassa 3.0-versiossa nopeus on 600 MB/s. 2004 julkaistiin eSATA (external SATA) kilpailemaan ulkoisten kiintolevyjen jo olemassa olevien USB ja FireWire liitännöiden kanssa. (Harddrivesecrets). (Kuva 10.)



Kuva 10: SATA:n kehitys.

6.4.4 SCSI

SCSI (Small Computer System Interface) on SASI:n (Shugart Associates System Interface) ja NRC Corporationin 1981 kehittämä standardi tiedon välittämiseen tietokoneen ja oheislaitteiden välillä. SCSI:a käytetään yleensä kiintolevyjen ja nauha-asemien liittämiseen tietokoneeseen. Tietokoneessa täytyy olla SCSI-ohjain, että siihen voi liittää SCSI-laitteen. SCSI on kehittynyt vuosien aikana ja siitä on julkaistu useita eri versioita. Vuodesta 2003 lähtien on ollut vain kolme SCSI standardia, SCSI-1, SCSI-2 ja SCSI-3. SCSI:ssa käytettiin aluksi rinnakkaista tiedonsiirtomenetelmää. Vuodesta 2008 julkaistiin SAS (Serial Attached SCSI), jossa tiedonsiirto muutettiin sarjamuotoiseksi. Tällä muutoksella saatiin nostettua tiedonsiirtonopeutta oleellisesti, joka on tehnyt SCSI:sta suositun liityntäväylän palvelimissa. (DataPro). (Kuva 11.)

Liityntä	Väylänopeus	Väyläleveys	Kaapelin enimmäispituus	Laitteiden enimmäismäärä
SCSI	5 Mt/s	8 bittia	6 m	8
Fast SCSI	10 Mt/s	8 bittia	1,5-3 m	8
Wide SCSI	20 Mt/s	16 bittia	1,5-3 m	16
Ultra SCSI	20 Mt/s	8 bittia	1,5-3 m	5-8
Ultra Wide SCSI	40 Mt/s	16 bittia	1,5-3 m	5-8
Ultra2 SCSI	40 Mt/s	8 bittia	12 m	8
Ultra2 Wide SCSI	80 Mt/s	16 bittia	12 m	16
Ultra3 SCSI	160 Mt/s	16 bittia	12 m	16
Ultra-320 SCSI	320 Mt/s	16 bittia	12 m	16
iSCSI	IP-verkko	N/A	N/A	??
SAS	375 Mt/s	1 bittia	8 m	16,256

Kuva 11: SCSI: kehitys ja erilaiset liityntätavat.

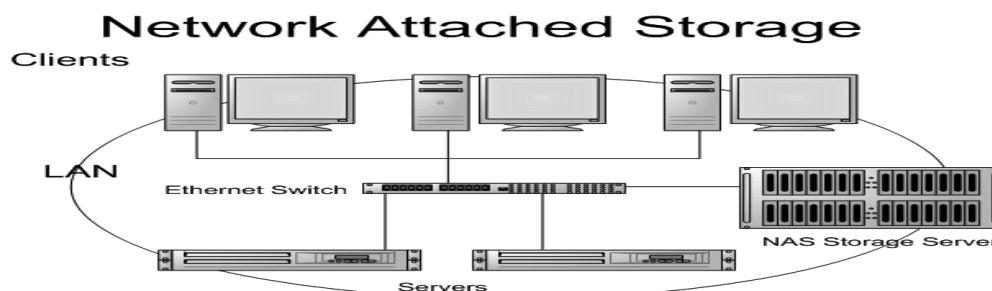
6.5 Verkkokiintolevyt

NAS-laitteet (Network Attached Storage) ovat toiminnaltaan yksinkertaisia pc-palvelimia, joiden tehtävänä on jakaa levykapasiteettia lähiverkon työasemille ja palvelimille. NAS-palvelimet ovat yksinkertaisia ja nopeita asentaa. NAS-palvelin liitetään lähiverkkoon verkkojohdolla ja sen hallinnointi tapahtuu internet selaimella. Palvelin on myös mahdollista määrittää lähettämään sähköpostiin ilmoituksia virheistä laitteen toiminnassa. NAS-palvelimet on kehitetty pääasiassa vain tietojen tallennukseen ja tämä kapea toiminnallisuus lisää niiden toimintavarmuutta. (Kuva 12.)

NAS koostuu yhdestä tai useammasta kiintolevystä. Palvelinten vikasietoisuutta parannetaan RAID-tekniikalla (Redundant Array of Independent Disks). RAID-tekniikka jakautuu seitsemään erilaiseen tekniikkaan, RAID 0 - RAID 6. Yleisimmät käytössä olevat tekniikat ovat RAID 0, RAID 1, RAID 1+0 (RAID 10), RAID 5 ja RAID 6. (Strom 2001, 1-3).

RAID 0 on tekniikka, jossa monta kiintolevyä yhdistetään niin, että ne näkyvät yhtenä tallennustilana. Data kirjoitetaan kaikille levyille lomittaen (striping) niin, että se jakautuu tasaisesti kaikille levyille. Jos yksi levy hajoaa, kaikki data häviää. RAID 1 tekniikassa data kirjoitetaan kahdelle tai useammalle levyille samaa aikaa. Tätä kutsutaan levyn peilaamiseksi (mirroring). Tässä tekniikassa levyn hajotessa tieto säilyy, koska ne löytyvät toiselta peilatuselta levyiltä. RAID 1+0 tekniikassa yhdistetään RAID 0 ja RAID 1 tekniikat, jonka avulla saadaan parannettua vikasietoisuutta. Tekniikka tunnetaan myös nimellä RAID 10.

RAID 5 on muita tekniikoita monimutkaisempi ja vaatii toimiakseen vähintään 3 kiintolevyä. Etuna on, että yksi levy voi hajota ilman, että tietoja menetetään. Ideana on, että tieto kirjoitetaan levyille hajautetusti niin kuin RAID 0-tekniikassa. Normaalin datan lisäksi levyille tallentuu pariteettidataa, jonka avulla tiedot pystytään palauttamaan yhden levyn hajotessa. Pariteettidata vie tilaa yhden pakassa olevan kiintolevyn verran eli esimerkiksi 3 x 200 gigatavun levyn tallennustila näkyy ulospäin 400 gigatavuna. RAID 6 toimii samalla tavalla, kuin RAID 5. Erona on, että kaksi levyä voi hajota ilman, että tietoja häviää. (Vadala 2002, 17-28).



Kuva 12: NAS:in liittäminen yrityksen verkkoon.

7 Tutkittujen vaihtoehtojen vertailu

Seuraavaksi vertaillaan varmistukseen valittuja menetelmiä. Valinnassa oleellimmat huomioon otettavat asiat ovat ratkaisun helppokäyttöisyys, luotettavuus, laajennettavuus ja kustannukset. Näiden kriteerien ja tutkimuksen perusteella valitaan parhaiten toimiva kokonaisuus. Valinnan apuna käytetään kahta menetelmää, benchmarkingia ja Kepner & Tregoe ongelmanratkaisumallia.

7.1 Varmistustekniikoiden benchmarking vertailu

Benchmarkingin avulla mitataan ja analysoidaan tuotteiden, palvelujen ja prosessien suorituskykyä. Benchmarkingin tavoitteena on oman organisaation ja oman toiminnan kehittäminen selvittämällä, mitkä ovat parhaita olemassa olevia toimintatapoja ja menetelmiä, vertailemalla niitä keskenään ja omiin toimintoihin sekä soveltamalla löydettyjä asioita oman yrityksen toimintaan. Tässä tutkimuksessa vertailun mittareina käytetään menetelmien hyviä ja huonoja puolia (Pros & Cons) (Niva & Tuominen 2005, 5-7).

7.1.1 Etävarmistus

Helppokäyttöisin vaihtoehto olisi varmasti etävarmistus. Varmistus tapahtuisi automaattisesti verkkoyhteydellä ja kopiointin voisi ajoittaa työpäivän jälkeen. Tiedot saa myös heti pois yrityksen tiloista. Tietojen kopiointi on palveluntarjoajan vastuu suorittaa ja varmistaa, että kopiot on tehty ja, että ne tehdään ajallaan ja oikeista tiedoista. Palveluntarjoajan palveluihin kuuluu myös usein tukipalvelu, johon kuuluu palvelun asennus ja tuki asennuksen jälkeen.

Varmistettavan tiedon määrä voi kuitenkin aiheuttaa ongelmia. Etävarmistuksen käyttäminen saattaisi aiheuttaa lisäkustannuksia, koska verkkoyhteyden nopeuttaa saattaisi joutua nostamaan. Datan kopioiminen verkkoyhteyden kautta on hidasta, jos yhteys ei ole tarpeeksi nopea. Kopioitava datamäärä saattaa myös rajoittaa palveluntarjoajan valintaa, koska monet palvelua tarjoavat yritykset rajoittavat datan maksimimääräksi 100 gigatavua.

Etävarmistuksen hintaan vaikuttaa seuraavat asiat:

- kopioitavan tiedon määrä,
- varmuuskopioitavien tietokoneiden ja palvelinten määrä,
- säilytettävien kopioiden määrä,
- tietojen säilyttämisen pituus ja
- mahdollinen käyttöönottopalvelu.

Tutkimuksen kautta löysin yhden yrityksen, joka suoraan antaa hinnan teratavun tallennukselle. Hinta on 600 €/kk. Kopioitavaa dataa on noin 750 gigatavua eli hinnaksi tulisi noin 500 € kuukaudessa. Vuodessa hinnaksi tulisi noin 6000 €. Hinta sisältää tietojen kopioinnin ja säilytyksen.

Etävarmistus		Hyvät puolet		Huonot puolet
		Helppokäyttöisyys		Suurien tietomäärien varmistus voi aiheuttaa ongelmia
		Tiedot heti pois yrityksen tiloista		Kustannukset
		Toimii automaattisesti		
		Ei vaadi lisälaitteita		

Taulukko 2: Etävarmistuksen vertailua.

7.1.2 Nauha-asetat ja nauhat

Nauha-asemia on käytetty pitkään varmuuskopioinnissa. Suuriin tietomääriin nauha-asetat ja nauhat sopivat hyvin niiden hyvän tallennusnopeuden takia. GeoUnion Oyn tapauksessa nauha-asema on jo hankittu eli kustannuksia aiheuttaisi vain siihen hankittavat nauhat. Nauhojen käytön hyväksi puoleksi voidaan myös laskea se, että nauhat ja etenkin niiden sisältämät tiedot saadaan helposti vietyä pois yrityksen tiloista.

Nauha-aseman käyttäminen ainoana ratkaisuna tuntuu kuitenkin jotenkin kömpelöltä. Nauhoille on myös hankittava erillinen säilytyspaikka ja niiden vaihtoon täytyy osoittaa henkilö. Tämä taas aiheuttaa sen vaaran, että nauha esimerkiksi unohtuu vaihtaa. Vaihtoehtoisesti nauhan säilytyksen ja nauhan vaihdon voi tilata palveluna. Tämä taas lisää kustannuksia. Nauhoilta on myös hidasta tuoda tietoja takaisin eli ainakin osa tiedoista olisi hyvä säilyttää yrityksen tiloissa nopeaa palautusta varten esim. ulkoisilla kovalevyillä.

Yrityksen omistama nauha-asema tukee LTO 4-tekniikkaa. Yhden tarvittavan tallennuskapasiteetin omaavan nauhan hinta on noin 60 euroa kappale. Jos kopio otettaisiin kuukauden välein, maksaisivat nauhat noin 720 euroa vuodessa. Kahden viikon välein otetut kopiot tarkoittaisi noin 1500 euron vuosikustannuksia. Tähän pitäisi vielä lisätä mahdollisen ulkoisen säilytys-, ja kuljetuspalvelun hinta.

Nauha- asema		Hyvät puolet		Huonot puolet
		Nauha helppo kuljettaa turvaan		Tiedon takaisinsaaminen nauhalta hidasta
		Nopea tallennusnopeus		Erillinen säilytyspaikka nauhalle
		Käytetty pitkään varmuuskopioinnissa		Nauhojen vaihtaminen
		Tiedot saa pois yrityksen tiloista		
		Hinta		

Taulukko 3: Nauha-aseman vertailua.

7.1.3 Verkkokiintolevyt

Verkkokiintolevyjen (NAS) käyttö ainakin osana varmuuskopiointia tuntuu järkevältä. NAS-laitteiden sisältämät RAID-toiminnot tekevät niistä luotettavampia, kuin tavalliset kiintolevyt. Laite on myös helppo liittää jo olemassa olevaan yrityksen verkkoon. Hyviä puolia ovat myös niiden tarjoama levyn yhteiskäyttö ja se, että laitteet eivät vaadi kauhean suuria investointeja.

Ainoaksi ratkaisuksi varmuuskopioinnin suorittamiseen ei NAS-laitteista mielestäni kuitenkaan ole. Suurin ongelma on se, että laitteen joutuu sijoittamaan yrityksen tiloihin ja usein samaan tilaan muiden laitteiden kanssa. Tämä aiheuttaa suuren riskin tietojen häviämislle. Tiedot pitäisi saada kopioitua erikseen toiselle laitteelle esimerkiksi ulkoiselle kovalevyille, joka kuljetettaisiin pois yrityksen tiloista.

Verkkokiintolevyn tallennuskapasiteetiksi päätettiin 4 teratavua. Tämä kapasiteetti riittää hyvin tämänhetkisen datamäärän tallennukseen ja varaa jää vielä datamäärän kasvamiseen. Yrityksen oheislaitteet on hankittu Verkkokauppa.comista. Tämän takia selvitin laitteiden hintoja Verkkokauppa.comin tarjonnan perusteella.

4 teratavun kiintolevyjen hinnat vaihtelevat 500 eurosta 1500 euroon. Vaatimukset laitteelle ovat, että siinä on mahdollisuudet vähintään RAID 1 tekniikan käyttöön. Neljän teratavun verkkokiintolevyjä Verkkokauppa.comista löytyy 16 erilaista. Näistä voi saman tien karsia pois sellaiset NAS-laitteet, jotka eivät sisällä oikeita RAID-tekniikoita. Oikean laitteen valintaa saa myös helpotettua sillä, että karsii pois sellaiset laitteet, jotka sisältävät ominaisuuksia joita yritys ei tarvitse. NAS-laitteelta haetaan pääasiassa kuitenkin vain lisätallennustilaa ja helppokäyttöisyyttä. Karsinnan jälkeen valinta on tehtävä 7 eri laitteesta.

NAS	Hyvät puolet	Huonot puolet
	RAID-toiminto	Ei ainoaksi ratkaisuksi
	Liitettävyyys	Yrityksen tiloissa
	Ei suuria investointeja	
	Helppo ottaa käyttöön	

Taulukko 4: NAS vertailua.

7.1.4 Kiintolevyt

Kiintolevyjä käytetään osana tiedon tallennusta automaattisesti, koska tietokoneissa on kiintolevyt ja palvelinten verkkokiintolevyt ovat vain palvelimeen kiinnitettyjä kiintolevyjä. Kiintolevyjen hyvänä puolena voidaan pitää niiden helppokäyttöisyyttä. Ulkoiset tai sisäiset kiintolevyt harvoin vaativat minkäänlaista asennusta. Tämän takia niitä on helppo siirtää ja liittää koneesta toiseen. Kiintolevyt ovat myös halventuneet paljon lähiaikoina, minkä voi laskea niiden hyväksi puoleksi. Esimerkiksi 1 teratavun ulkoisen kiintolevyn saa jo alle sadalla eurolla (Verkkokauppa.com). Tämä tekee niistä varteenotettavan vaihtoehdon kopioinnin suorittamiseen. Useat kiintolevyt sisältävät myös valmiin ohjelman millä tehdä kopioinnista automaattista. Kiintolevyille luvataan myös pitkiä kestävyys aikoja.

Huonoiksi puoliksi voidaan laskea se, että ne jäävät toimiston tiloihin tai niille pitää hankkia erillinen säilytyspaikka. Jos niitä aletaan kuljettamaan pois yrityksen tiloista, tarkoittaa se lisäkuluja. Tämä tarkoittaisi uuden kiintolevyn ostamista tietyin väliajoin ja erillisen säilytyspaikan hankkimista tai vuokraamista. Kiintolevyt saattavat myös hajota helposti, vaikka niille luvataan pitkiä kestävyys aikoja.

Palvelimille on kertynyt tietoa jo sen verran paljon, että varmistamista varten ostettavan kiintolevyn koko on oltava tallennuskapasiteetiltaan vähintään 1.5 teratavua. Tämän kokoluokan kiintolevyt maksavat 80-200 €. Hintaan vaikuttaa eniten kiintolevyn liitännäismahdollisuudet. Tulevaisuutta ajatellen yrityksen hankkimasta levyistä niitä olisi löydettävä mahdollisimman paljon. Tämä nostaa hankittavan levyn hintaa noin 120 euroon. Levyjä olisi hyvä olla vähintään kaksi mahdollisen hajoamisen takia. Tämä nostaisi kustannukset noin 250 euroon, mikä tekisi tästä menetelmästä halvan vaihtoehdon.

Ulkoiset kiintolevyt	Hyvät puolet	Huonot puolet
	Helppokäyttöisyys	Pitää hankkia erillinen säilytyspaikka
	Liittäminen muihin laitteisiin	Kestävyys
	Hinta	
	Kestävyys	

Taulukko 5: Ulkoisten kiintolevyjen vertailua.

7.2 Varmistustekniikoiden Kepner & Tregoe vertailu

Kepner & Tregoen ongelmanratkaisumallin avulla selvitetään vastaako, varmistusmenetelmä sille asetettuja vaatimuksia. Menetelmän tarkoituksena on tukea päätöksentekoa. Aluksi päätetään päämäärä, jota menetelmällä halutaan saavuttaa. Sen jälkeen selvitetään vaatimukset, joiden perusteella valinta tehdään. Vaatimukset jaetaan kahteen ryhmään, pakollisiin ”Must” ja toivottaviin ”Want”. Seuraavaksi päätetään kumpaan ryhmään vaadittu ominaisuus kuuluu. Kun ”Must” ryhmän ominaisuudet on päätetty, tulevat loput ominaisuudet ”Want” ryhmään tärkeysjärjestyksessä. ”Want” ryhmään valitut pisteytetään asteikolla 0-10 ja pisteet lasketaan lopuksi yhteen (decision-making-confidence.com).

Tässä tapauksessa Kepner & Tregoen ongelmanratkaisumallin päämääräksi asetetaan yritykselle sopivan varmuuskopiointimentelmän valitseminen. ”Must” -vaatimuksia olivat jo aikaisemmin tärkeimmiksi ominaisuuksiksi määritellyt helppokäyttöisyys, luotettavuus, laajennettavuus ja kustannukset. ”Want” -ominaisuuksiksi määriteltiin toipuminen virhetilanteista ja turvallisuus, joiden kummankin painoarvoksi määriteltiin yhdeksän pistettä asteikolla 0-10.

MUST		Etävarmistus	Nauha-asemat	Verkkokiintolevyt	Kiintolevyt
Helppokäyttöisyys		x		x	x
Luotettavuus			x	x	
Laajennettavuus				x	x
Kustannukset			x	x	x

Taulukko 6: ”Must” ominaisuudet.

WANT	Painoarvo	Etävarmistus	Nauha-asemat	Verkkokiintolevyt	Kiintolevyt
Toipuminen virhetilanteista	9		x	x	
Turvallisuus	9	x		x	
Etävarmistus = 9					
Nauha-asemat = 9					
Verkkokiintolevyt = 18					
Kiintolevyt = 0					

Taulukko 7: "Want" ominaisuudet.

7.3 Kepner & Tregoe vertailun tulokset

Ongelmanratkaisumallin tuloksen mukaan paras vaihtoehto olisi verkkokiintolevyn käyttö tietojen varmistuksessa. Menetelmä täyttää "Must" -vaatimuksista kaikki ja saa korkeimman pistemäärän "Want" -ominaisuuksien pisteytyksessä. Vähiten "Must" -ominaisuuksista täyttää etävarmistus. Kiintolevyt täyttävät kolme neljästä "Must" -ominaisuudesta, mutta "Want" -ominaisuuksista ei yhtään. Nauha-asemat täyttävät kaksi neljästä "Must" -vaatimuksista ja "Want" -vaatimuksista yhden.

7.4 Päätösanalyysi

Vertailun perusteella kaikista vaihtoehtoista löytyy huonoja ja hyviä puolia. Toiset varmistusmenetelmät ovat helppokäyttöisempiä ja toisista taas löytyy loistavia ominaisuuksia varmuuskopiointia ajatellen. Ainoaksi ratkaisuksi yhdestäkään menetelmästä ei kuitenkaan ole vaan varmistus kannattaisi tehdä esimerkiksi kahden menetelmän yhdistelmällä. Paras vaihtoehto vertailun perusteella on NAS. Varsinkin RAID-ominaisuus tekee NAS:sta hyvän vaihtoehdon. Laitteen hankkiminen ei myöskään aiheuta suuria kustannuksia. Ainoaksi ratkaisuksi ei verkkokiintolevystä ole, koska tiedot jäävät varmistuksen jälkeen yrityksen tiloihin.

8 Ratkaisuehdotus

Tutkimuksen perusteella ehdotetaan seuraavaa menettelyä: varmuuskopiointi suoritetaan NAS-laitteella ja ulkoisilla kovalevyillä. NAS sisältää erittäin hyviä ominaisuuksia varmistusta ajatellen. Tärkeimpinä näistä ovat laitteen helppo käyttöönotto, helppo liitettävyys jo olemassa olevaan tietoverkkoon ja NAS-laitteen sisältämät RAID-toiminnot.

Tallennuskapasiteettia on myös tarpeen vaatiessa helppo kasvattaa. Data varmistettaisiin NAS:sta ulkoiselle kovalevyille, joka kuljetettaisiin pois yrityksen tiloista. Kopioimalla data ulkoisille kovalevyille ja kuljettamalla se pois yrityksen tiloista saadaan tiedon säilyvyyttä vielä parannettua.

NAS-laitteen kooksi ehdotetaan 4 teratavua. Tällä tallennuskapasiteetilla saadaan varmistettua kummatkin palvelimet. NAS-laitteeseen liitetään ulkoinen kovalevy, jolle varmistetaan tiedot NAS-laitteesta. Ulkoista kovalevyä vaihdetaan tietyin väliajoin ja se vietään pois yrityksen tiloista. Vaihto tehdään normaalin ylläpidon yhteydessä GeoUnion Oy:n it-tuesta vastaavan yrityksen toimesta.

Ratkaisu toteutetaan yhdessä GeoUnion Oy:n it-tuesta vastaavan yrityksen kanssa, joka myös vastaa ulkoisten kovalevyjen vaihdosta ja säilytyksestä. Yritys on toteuttanut aikaisemminkin vastaavia varmuuskopiointimenetelmiä. Tämän takia ehdotetaan, että myös tarvittavat laitteet hankitaan kyseiseltä yritykseltä. Laitteita ei kannata ostaa. Järkevämpi vaihtoehto on, että GeoUnion Oy vuokraa laitteet yritykseltä. Etuna on myös se, että yritys on testannut käyttämiään laitteita jo aikaisemmin ja voivat näin taata niiden toimivuuden. Tämä helpottaa myös laitteiden päivittämistä tulevaisuudessa. Ehdotan, että varmistus tehdään päivittäin NAS:lle ja kovalevyille. Kovalevyn vaihto tehdään kerran viikossa.

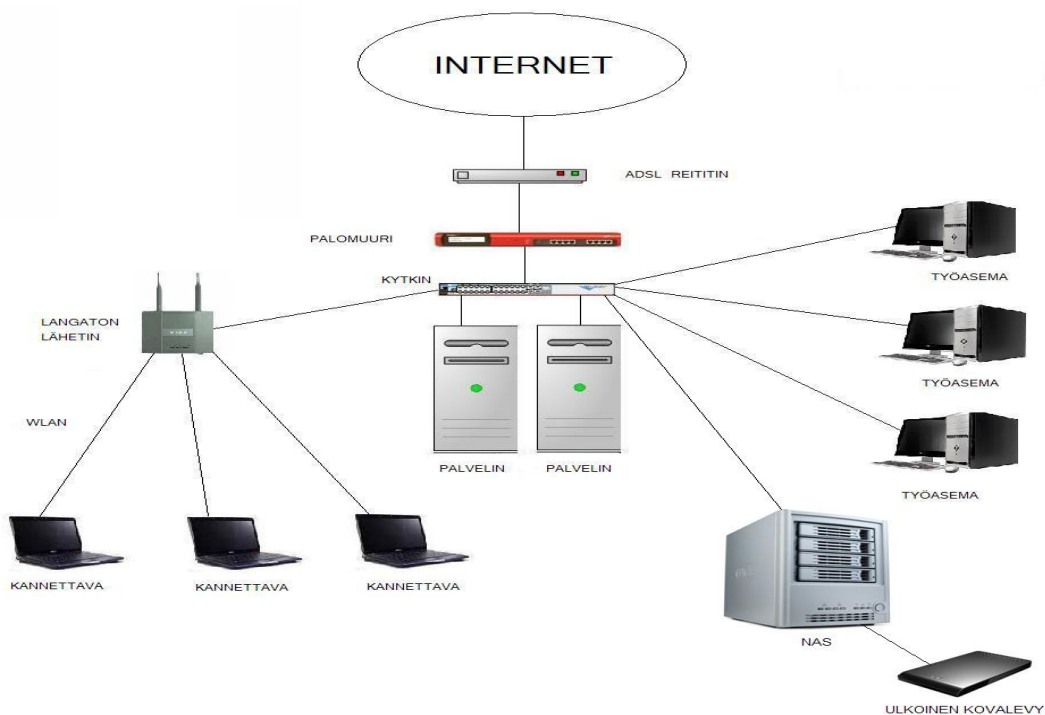
Palvelimen sisältämien verkkolevyjen tallennuskapasiteetti on loppumassa. Tämän takia ehdotan myös, että GeoUnion Oy lisää samalla yrityksen sisäverkkoa ylläpitävään palvelimeen lisää tallennustilaa.

9 Valittu ratkaisu ja kustannukset

Yrityksen varmuuskopiointi on päätetty toteuttaa ehdotetulla tavalla. Yrityksen palvelimeen on liitetty neljän teratavun NAS-laite, jolle varmistukset tehdään. Laitteesta tiedot siirretään ulkoiselle kovalevyllä, joka vaihdetaan ja viedään pois yrityksen tiloista. Palvelu on ostettu yrityksen it-tuesta vastaavalta yritykseltä. Lisäehdotukseni tallennustilan lisäämisestä on myös toteutettu. Samalla yritys päivitti palvelimen käyttöjärjestelmän uudempaan (Kuva 13).

Varmuuskopiointin kustannukset koostuvat laitteista ja asennukseen käytetystä ajasta. NAS-laite maksaa 58,40 €/kk ja ulkoiset kovalevyt 39,35 €/kk. Sopimus on tehty alustavasti 36 kuukaudeksi. Asennuksesta laskutettiin 99€ tunti ja siihen käytettiin aikaa kahdeksan tuntia. Vuodessa varmuuskopiointi tulee maksamaan yritykselle noin 1200 € vuodessa. Tähän on vielä lisättävä asennukseen käytetyn ajan aiheuttamat kustannukset. Lisätyönä tehty palvelimen käyttöjärjestelmän päivittäminen ja tallennustilan lisääminen nostivat kustannuksia huomattavasti, mutta tulevaisuutta ajatellen ne olivat välttämättömiä.

Haastattelun toinen osa tehtiin sen jälkeen, kun uusi varmistusmenetelmä oli otettu käyttöön. Sen perusteella yritys on ollut tyytyväinen valittuun menetelmään eikä sillä ole ollut mitään negatiivisia vaikutuksia yrityksen jokapäiväiseen toimintaan. Tähän mennessä ongelmilta on myös välttytty (Liite 1, osa 2).



Kuva 13: GeoUnion Oy:n sisäverkko, johon on liitetty NAS.

10 Kehitysprojektin yhteenveto

Tätä työtä lähdettiin tekemään, koska yrityksen varmuuskopiointia ei ollut toteutettu riittävän hyvällä tavalla. Työn tarkoituksena oli tutkia ja suunnitella yritykselle sopiva varmuuskopiointimenetelmä. Aluksi selvitettiin yrityksen nykyinen varmuuskopioinnin tila. Tämän jälkeen päätettiin tutkittavat menetelmät ja selvitettiin yrityksen vaatimukset menetelmille. Teoria osuudessa käytiin läpi valittujen menetelmien ominaisuuksia ja selvitettiin tarkemmin niiden toimintaa. Menetelmiä vertailtiin käyttämällä apuna kahta menetelmää, Benchmarkingia ja Kepner & Tregoen ongelmanratkaisumallia. Työ eteni suunnitelman mukaan ja tulokseksi saatiin toimiva ja tämän hetken tarpeen kattava varmuuskopiointi.

Täysin varmaa ja lopullista varmuuskopiointiratkaisua ei varmasti ole olemassa. Tämän takia yrityksellä on tulevaisuudessa edessä valitun menetelmän kehittäminen tai mahdollisesti toisenlaisen menetelmän käyttöönotto. Nykyinen ratkaisu kuitenkin kattaa hyvin tämän hetken tarpeen. Tutkimus oli hyödyllinen myös sen takia, että samalla saatiin päivitettyä yrityksen palvelimen käyttöjärjestelmä ja lisättiin tallennuskapasiteettia. Nämä olisivat olleet kuitenkin edessä tulevaisuudessa.

Lähteet

Hakala, M. Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. 1. painos. Jyväskylä: Docendo Finland Oy.

Jaakohuhta, H. 2003. Tietojärjestelmien luotettavuus. 1. painos. Helsinki: Edita Prima Oy.

Jordan, E. & Silcock, L. 2006. Strateginen IT-riskien hallinta. Helsinki: Edita Prima Oy.

Järvinen, P. 2002. Tietoturva ja yksityisyys. 1. painos. Jyväskylä: Docendo Finland Oy.

Kuusela, H. & Ollikainen, R. 2005 Riskit ja riskienhallinta. Tampere: Tampereen yliopistopaino OY - Juvenes Print.

Laaksonen, M. Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Oy Nordprint Ab.

Mäntysalo, V. Kehityspäällikön haastattelu 2010. GeoUnion Oy, Helsinki.

Niva, M. & Tuominen, K. 2005. Benchmarking käytännössä. Turku: Oy Benchmarking Ltd.

Paavilainen, J. 1998. Tietoturva. Jyväskylä: Gummerus Kirjapaino Oy.

Ruohonen, M. 2002. Tietoturva. 1. painos. Jyväskylä: Docendo Finland Oy.

Vadala, D. 2003. Managing RAID on LINUX. 1. painos. Yhdysvallat: O'Reilly & Associates, Inc.

DataPro. All About SCSI.

Viitattu 11.7.2010. http://www.datapro.net/techinfo/scsi_doc.html

Decision-making-confidence.com. Kepner Tregoe Decision Making.

Viitattu 18.4.2011. <http://www.decision-making-confidence.com/kepner-tregoe-decision-making.html>

Geo Union Oy. 2010.

www.geounion.fi

Harddrivesecrets.com. Everything you need to know about Serial ATA.

Viitattu 10.7.2010. <http://www.hardwaresecrets.com/article/27>

Hewlett-Packard 2010. Tape storage & media.

Viitattu 2.7.2010. <http://h18006.www1.hp.com/storage/tapestorage/index.html?psn=storage>

Knowledgerush. Integrated Drive Electronics.

Viitattu 10.7.2010.

http://www.knowledgerush.com/kr/encyclopedia/Integrated_Drive_Electronics/

MANUAALI.FI. Kiintolevy.

Tulostettu 9.7.2010. <http://manuaali.fi/tietokone/tietokoneen-osat/kiintolevy.html>

McIntosh J. 2009. SDLT Tape Technology.

Viitattu 3.7.2010. <http://www.ex-designz.net/articleread.asp?aid=5171>

PCGUIDE. Hard Disk Drives.

Tulostettu 9.7.2010. <http://www.pcguides.com/buy/des/compHDD-c.html>

PCTECHGUIDE. AIT Technology.

Viitattu 3.7.2010. http://www.pctechguide.com/35Tape_AIT_technology.htm

Quantum Corporation. Digital Linear Tape (DLT) Technology and Product Family Overview. Tulostettu 4.7.2010.

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.39.137&rep=rep1&type=pdf>

SearchStorage.com 2010. Online backup.

Viitattu 11.7.2010.

http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci1151930,00.html

SKOL RY 2010. Sopimusehdot (KSE 1995).

Viitattu 1.7.2010.

<http://www.skolry.fi/easydata/customers/skolry/files/hankinta/10574.pdf>

Sony 2010. Digital Data Storage.

Viitattu 2.7.2010. <http://b2b.sony.com/Solutions/subcategory/recordable-media/storage-media/dds>

ULTRIUM LTO. LTO Technology.

Viitattu 8.7.2010. <http://www.ultrium.com/technology/index.html>

Kuvat

Kuva 1: Geo Union Oy:n tietoverkon rakenne.	12
Kuva 2: HP:n Storageworks Ultrium nauha-asema.	18
Kuva 3: Kaavio DDS:n tiedonsiirtonopeuden kehittymisestä.	19
Kuva 4: Super Digital Linear Tape.	20
Kuva 5: Kaavio AIT:n kehityksestä.	21
Kuva 6: SAIT:n kehittyminen.	21
Kuva 7: LTO-tekniikan suunniteltu kehittyminen.	22
Kuva 8: Esimerkki etävarmistuksen toteutuksesta.	23
Kuva 9: IDE:n liitännät ja liittäminen tietokoneeseen.	24
Kuva 10: SATA:n kehitys.	24
Kuva 11: SCSI: kehitys ja erilaiset liityntätavat.	25
Kuva 12: NAS:in liittäminen yrityksen verkkoon.	26
Kuva 13: GeoUnion Oy:n sisäverkko, johon on liitetty NAS.	34

Taulukot

Taulukko 1: Riskit.	15
Taulukko 2: Etävarmistuksen vertailua.	28
Taulukko 3: Nauha-aseman vertailua.	29
Taulukko 4: NAS vertailua.	30
Taulukko 5: Ulkoisten kiintolevyjen vertailua.	31
Taulukko 6: "Must" ominaisuudet.	31
Taulukko 7: "Want" ominaisuudet.	32

Liitteet

Liite 1. Kehityspäällikkö Ville Mäntysalon haastattelu	4
--	---

Haastattelu Osa 1

Haastateltavan nimi: Ville Mäntysalo

Työnimike: Kehityspäällikkö

1. Kuinka kauan olet työskennellyt GeoUnion Oy:ssä?

Kesätöissä olen ollut yhtiön perustamisesta lähtien, eli noin 16 vuotta sitten ensimmäisen kerran. Vakituisesti aloitin 2004 kesällä kun sain omat opintoni suoritettua loppuun.

2. Miten paljon olet ollut mukana yrityksen tietoverkon rakentamisessa?

Alku aikoina en ollut tekemisissä ollenkaan. Kun 2007 siirryin maastotöistä työnjohtoon ja toimistolle töihin niin verkko oli jo toiminnassa. Henkilö joka tuolloin vastasi verkosta siirtyi muualle töihin 2008 vuoden kesällä ja verkon ylläpito jäi vastuulleni.

3. Miksi varmuuskopiointia on lähdetty suunnittelemaan?

Kaikki meidän valmiit työmme säilötään nykyään sähköisessä muodossa ja meillä on velvollisuus pitää ne tallessa 10 vuotta työn valmistumisesta. Tämä ja yrityksen kasvaminen viime aikoina ovat aiheuttaneet sen että nykyiset menetelmät eivät enää ole riittävät.

4. Miten tiedonvarmistus toimii tällä hetkellä?

Tällä hetkellä tiedot siirtyvät öisin talteen ulkoiselle levyasemalle. Työtekijöiden omat tiedostot ja sähköpostit kopioidaan verkon yli ja järjestelmästä on otettu myös varmistukset niin, että se pystytään palauttamaan sen kaatuessa.

5. Onko tietoa joskus kadonnut ja miten tällaisessa tilanteessa on toimittu?

Ei ole tähän mennessä kadonnut aineistoa palvelimelta. Ainoastaan mittauslaitteiden muistikorteilta mutta niistä on saatu tiedot palautettua ohjelmistojen avulla.

6. Mitä vaatimuksia yrityksellä on varmuuskopioinnille?

Uuden varmuuskopiointimenetelmän haluaisimme olevan mahdollisimman automaattinen. Niin ettei se aiheuttaisi lisää sisäistä työtä. Toisekseen tarvitsisimme ulkoisen säilytyspaikan varmuuskopioituille tiedoille, poissa yrityksen tiloista. Emme kuitenkaan halua että vanhat työmme siirtyvät vaikeasti tavoitettaviksi sillä joudumme usein palamaan jopa viisi vuotta vanhojen töiden pariin.

Tärkeätä olisi myös, että menetelmä olisi helppokäyttöinen, luotettava ja turvallinen. Tulevaisuutta ajatellen olisi myös hyvä, jos menetelmää olisi mahdollista helposti muokata ja laajentaa tarvittaessa.

7. Kuinka tärkeänä pidät tietojen varmistamista yritykselle?

Tietojen varmistaminen on erittäin tärkeää meidän alan yrityksille. Kaikki työmme säilötään ja tehdään nykyään sähköiseen muotoon. Pelkästään tiedon säilömisvelvollisuus on 10 vuotta. Lisäksi joudumme usein palaamaan vanhojen töiden pariin vuosien jälkeenkin. Olisi erittäin noloa jos joutuisi sanomaan että tiedot ovat hävinneet.

Osa 2

8. Onko uusi varmuuskopiointimenetelmä vaikuttanut yrityksen toimintaan?

Ei ole vaikuttanut työn tekemiseen. Varmuuskopiointi tapahtuu automaattisesti yön ja viikonloppujen aikana. Päivällä ei edes huomaa että muutoksia olisi tapahtunut. Henkisellä puolella tietysti helpottaa kun asia on viimein saatu hoidettua. Tulee nukuttua öisin paremmin, kun tietää että varmuuskopiointi on kunnossa.

9. Onko yrityksessä oltu tyytyväisiä uuteen menetelmään?

Vielä ei ole tullut valituksia keneltäkään varmuuskopiointiin liittyen. Niin kauan kun kukaan ei valita on kaikki varmasti kunnossa.

10. Onko ollut ongelmia ja jos on niin mikälaisia?

Tähän mennessä on kaikilta ongelmilta välttytty. Tosi testaus tapahtuu vasta kun ensimmäisen kerran jotain aineistoja häviää.